Wireless Mesh Network OAM Architecture

Malaz Kserawi, Sangsu Jung, and June-Koo Kevin Rhee.
Information and Communications University, 119 Munji-ro Yuseong-gu Daejeon, 305-732, S. Korea
{malaz, ssjung, rhee.jk}@icu.ac.kr

***Abstract* — Wireless Mesh Networks (WMNs) have been expected to be future commercial service-grade networks. OAM (Operations, Administration, and Maintenance) in wired networks is an important tool to guarantee a reliable network performance, WMNs needs such a tool to meet the service providers requirements, and to handle mobility problem. We propose a fundamental architecture of wireless mesh network OAM to maintain a certain level of service by handling mobility, in addition to fault management and performance management.**

***Keywords* — Wireless mesh network, operation administration and maintenance, continuity check, mobility management.**

1. Introduction

Operations, Administrations and Maintenance (OAM) in general, provides management functions such as fault detection, reporting, and isolation [1][2]. Other functions are for performance and security management. Even though wireless mesh networks need OAM function to be successfully deployed as commercial networks, there have been few trials on the aspect of service providers. Distinctively from wired networks, wireless mesh networks have their own specific generic characteristics due to the shared natured of the wireless medium, large-scale multi-hops, and the traffic characteristics as presented in Table 1.

To ensure the required service level and to meet the requirements in the contracts among users, network providers, and service providers in commercial WMNs, an OAM function should be well designed.

The first step toward a provider-level WMN service is to manage faults. That is, any fault happens in the network should be detected and reported to a manager; the manager verifies this fault and finally isolate it within a reasonable time bound. Wired OAM provides this function as defined by ITU-T [2].

We develop a WMN-specific OAM architecture (WMN-OAM) to deal with fault management for a service-grade wireless mesh network. The proposed functions include continuity check, loop back, and link trace. Continuity check is performed by exchanging periodic messages between network entities to guarantee network continuity; loop back verifies faults between two network nodes; and link trace localizes a fault in a specific path.

Another role of WMN-OAM is performance management. Especially, it considers the nature of wireless medium, client mobility, and limited bandwidth. Performance monitoring plays a significant role in detecting network failures, analyzing a network, and optimizing protocols on the perspectives of network manager and network designer.

We suggest a performance management guideline and show an example of network performance parameters which is residual bandwidth.

The paper is organized as follows: Section 2 explains the architecture of WMN-OAM, in section 3 the fault management of WMN-OAM is introduced based on the management tree model. Performance management is discussed in section 4, and section 5 discusses future directions of WMN-OAM. Finally, section 6 concludes the paper.

Table 1. Comparison between wired networks and WMNs.

	Wired Networks	Large-Scale WMNs
Link	Stable	Unstable
Collision Domain	Limited to a point-to-point link	Open within a coverage area
Preferred Routing	Hop-count based Routing	Static routing
Mobility	None	Client Mobility
Bandwidth	High	Limited
Power	Always available	Limited for clients

This work was supported in part by the Korea Research Foundation Grant funded by the Korean Government (KRF-2008-313-D00685).

2. Wireless Mesh Network-OAM Layering

Similar to Ethernet OAM layers, wireless OAM layers can be defined. Fig. 1 shows how OAM domains are classified into three types; the customer, provider, and operator domains. Each WMN-OAM domain is defined as a network or a sub-network that belongs to a specific administrative entity. The reason behind a layering approach is to confine WMN-OAM flows and responsibilities within specific domains and to allow business relationships and accountability. Each domain should handle its own OAM capability independently, therefore; domains should not overlap with each others.

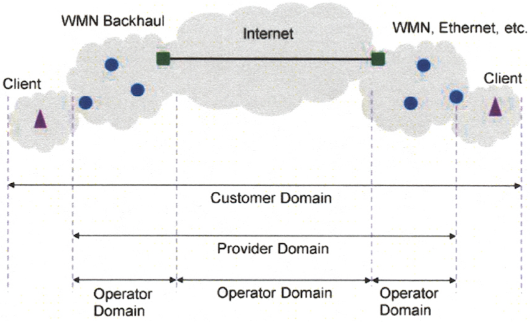

Figure 1. WMN-OAM domains.

These domains are responsible for fulfilling the contracts between each others. For example, a provider domain should manage to fulfill the contracts with clients for end to end services. Similarly, an operator domain should provide specific services for providers. A service in a specific domain does not necessarily mean that it is established between two separate networks as in both sides of Figure 1, but it could exist in one network, like mobility management within a network which exists in a customer domain and still needs the credibility of the provider domain.

3. Fault Management of WMN-OAM

In a wireless mesh network, it is hard to define maintenance entities and continuity check messages as in wired networks due to the different nature of WMN. In order to guarantee the continuity of all nodes in the network, an OAM system is required to detect, and report faults to a manager to take an action. For this purpose, we consider a management model, especially, a tree-based model to manage the health efficiency in a hierarchic approach. In this management model we use continuity check, loop back, and link trace messages.

Management tree: in order to contain all nodes, a tree should be built that contains all nodes in a segment, each segment contains one gateway, and a network contains number of segments similar to the number of gateways. Each node is included in the segment with the gateway that is assigned for this node by a routing protocol.

Segments are represented in hierarchy according to parents, children model, each node is assigned one parent and a number of children as in Figure 2. We choose the gateway to be the segment manager since it is usually the decision maker, it has information about the network and because it is connected directly to internet which could be useful for web network monitoring system such as systems in [4][5][6].

Continuity Check (CC): CC messages are periodic messages sent from a network entity to another entity. The period between two consecutive CC messages varies 3.3 ms to 10 seconds.

CC messages should be sent by all network nodes to the manager in our model, this might lead to a large overhead especially around the gateway where will be a number of messages similar to the number of nodes in the network every 1 second. For this reason, we propose the following procedure: CC messages start from segment borders (nodes with no children) and transmitted to their parents informing them that connection is functioning well. Parent nodes, like node 9 in Figure 2 and 3, waits for CCs from all children (10 and 11) and aggregate these messages before forwarding them, when node 9 is sure that all nodes beneath it are well connected, it sends one CC message to its parent (node 6), this message informs 6 that nodes 9, 10, and 11 are still connected, when 6 receives this CC and a similar one from node 7, it is now ready to inform the gateway that all of this cluster is working properly (node 6 and all nodes beneath it), this is also done by one CC message from 6 to gateway. This procedure reduces the received messages by gateway from number of nodes in the network to number of neighboring nodes, i.e. from 11 MSG/second to 3 MSG/second in our simple example. Moreover, this procedure is a good solution to allow scalability in our mesh network.

If node 6 did not receive CC message from 7 during the designated period, it assumes that a failure happened, and it includes this information in the next CC message to inform the manager about this event to take any necessary action. The manager does not consider this event as a failure from the first time, because the absence of CC message might be caused by a different reason. Thus, it waits for 3 consecutive alerts then it makes the decision that a fault happened.

CC messages are one-way messages from nodes to gateway that are triggered by one request message from the gateway. Nodes will keep transmitting unless they receive a CCstop message from manager.

Loop Back: As CC messages detects and report faults, Loop Back (LB) messages play the role of verifying these faults. LB message is established on a manager demand, automatically after continuity failure, or periodically, it is sent from manager to any network node. The manager expects a reply from this node to check connectivity. Moreover; it could be used to check the round trip time between a network node and the gateway.

Link Trace: the role of LT message is to locate a fault in a specific path in case of continuity failure, it is sent on demand by manager to a network node. The manager receives one LT

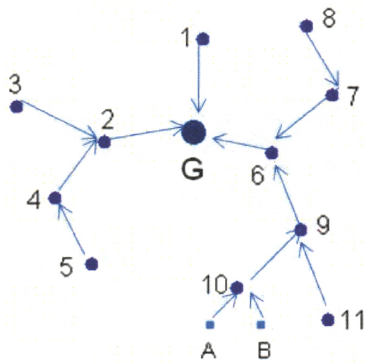

Figure 2. CC messages in mesh topology A, B: mobile hosts.

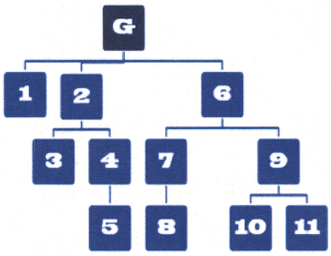

Figure 3. Management tree according to parents, children classification.

reply from each in-path-node along the path to the target node. The manager checks the replies received from nodes, and detects the missing replies to know the location of the failure.

In the CC case, the manager sends one CC request and receives many replies periodically until it sends a CCstop message. In the LB case, the manager sends a request and expects only one reply, while in the LT case, the manager sends one LT request, and expects to receive replies from all intermediate nodes in the path to the destination node.

This tree management scheme with CC, LB, and LT messages allow us to detect, report, verify, and localize faults in any kind of WMN. This network layer design gives better performance than application layer design as in [9]. Moreover, aggregation technique in CC messages allows scalability for large scale WMN.

Mobility management: CC messages can handle information related to mobile hosts, such as absence of a client, or new entry, in networks that requires information about the connected clients in its database. It could also provide location information for mobile hosts. When a mesh access point loses a connection or detects a new connection with a client, it includes this event in the next CC to inform the manager about this absence/entry. When a mobile host moves out of the coverage area of its connected access point, this access point will report the absence of the mobile host. This information however, is not enough to know the status of the mobile host whether this event is a failure or mobility. Our model provides a good solution for this problem with the help of a common parent. A common parent is a node that contains two access points beneath it in the management tree, and these two access points are the old and the new access points connected to a moving client. For example when the client B moves from access point 10 to 11, the common parent is node 9. Common parent could be the first parent, second parent or any higher degree parent, in some cases it might be the gateway. The role of this common parent is to distinguish mobility and failure. Usually node 9 waits for CC messages from nodes 10 and 11 to aggregate them and sends one CC message to 6, if the CC message from node 10 contains the absence of a client B, and CC message from node 11 contains a new entry of the client B node 9 (the common parent) will make a decision that this event is mobility not a failure. It will send an Alarm suppression message to node 10, to stop reporting this event. In the CC message generated to its parent (node 6) , instead of including both events (absence and new entry of B), it will include a movement event in the CC message or no new event in case if the manager does not need this information. In case if node 9 received only an absence event in the CC message from node 10 and no new event from node 11, it will include this event in the CC message to be delivered to the manager. If the manager received 3 consecutive absence events, it considers a failure happened and will take any necessary action.

4. Performance Management of WMN-OAM

Performance monitoring: The complexity of a large-scale multi-hop mesh network makes performance monitoring more difficult and yet more important. The importance of monitoring has many aspects; one example is to help the network in controlling performance and in making decisions, to guarantee a specific level of a service for users. Analyzing information obtained by monitoring can help network operators to understand the network status, topology, unnoticed problems, and other conclusions that make them able to increase the network efficiency significantly. Another use for monitoring information is that it can help designers understand the behavior of a network and thus improve protocols and services accordingly.

Information from nodes such as network status, traffic, bandwidth, and many others, should be gathered and delivered to the manager and stored in an information database. According to manager preferences and network types, different kinds of information could be chosen to be measured and delivered such as link quality [8], data flow, etc. In our architecture, it makes sense to use CC messages to deliver some kind of information that needs to be updated periodically, to reduce the overhead of WMN-OAM.

Monitored information should be classified into two categories, time dependent information, and time independent information. Time dependent information are the data that needs to be monitored and processed in real-time such as monitoring the throughput of a specific flow. This kind of information should be delivered instantly and periodically. Usually this kind of monitoring has higher priority. As for time independent information, it has lower priority since it does not have time constraints. An example of time independent information is the location of a specific mesh access point. The management system should be able to distinguish between those two kinds to be processed separately [9] and to consider priority.

Performance optimization: Performance information obtained by WMN-OAM can be used for traffic engineering in a network, and hence optimize performance. Traffic engineering functions can utilize the data to overcome performance shortcomings, or to apply possible enhancements. We propose one kind of performance monitoring for performance management in WMN-OAM, which is residual bandwidth at network nodes. Understanding how bandwidth is used along all network area makes the network able to make better traffic plans and locate areas with high traffic, and moreover, it can help finding a better location for the gateway. We however, will give an example of utilizing this information to improve performance; this example is making admission control decisions for new flows based on residual bandwidth information.

To calculate residual bandwidth at network nodes, we can use MARIA model [7], in this model, each node calculates the bandwidth of the flows that are passing through it and through the neighboring nodes and sum them together, after calculating the bandwidth used by these flows, the result is subtracted from the link capacity, the final result is the available bandwidth that can be used by this node. After calculating the residual bandwidth by each node, the information should be delivered to the manager (the gateway) periodically, to keep the manager updated with the bandwidth status of the nodes. To avoid extra overheads, we use CC messages to handle this delivery responsibility, since each node is already sending periodic CC messages to the manager, it can include the residual bandwidth information in these CC messages to be delivered to the periodically and with a low overhead. As the manager has an updated list of residual bandwidth in the database, we can show how this information could be useful to improve performance with an example.

In commercial WMNs, VoIP or video streaming requires a specific level of QoS to be provided. When a call request comes from wired internet to a network node through the gateway, the gateway should be able to decide whether the route assigned by the routing protocol is able to handle this call with the required performance or not; otherwise, the call may suffer from poor performance, and can affect the performance of other established flows in the network as well. Thanks to the information about residual bandwidth, the manager can check the path nodes along the route, and check their available bandwidth to see which node has the lowest residual bandwidth, and then, compare this value with the bandwidth required for the call. If it is enough to handle the call, it gives permission for the call to start, otherwise it will deny the call and avoid giving bad performance for this call and for other established calls. For better results, this algorithm could negotiate with the routing protocol to find a suitable path for this call, in our situation however; we ignore this part since it is not related with wireless OAM objectives.

5. Future Directions

In order to provide a complete fault management model; we need to provide a technique for fault recovery and isolation to eliminate fault propagation. In performance management, we proposed one kind of performance parameters to monitor and deliver using CC messages, however; in our future WMN-OAM model we should define the parameters to monitor, and a method for delivery since using CC messages might not be the best solution to deliver many parameters. Security management which is beyond the scope of this paper, is an important tool in OAM and should exist on our model to guarantee the safety of WMN, thus; we will investigate unique security threats in WMN compared to wired ones to implement a suitable safety models.

Some ICMP and SNMP functions are already implemented in WMNs due to their importance, we will try to optimize them and integrate them with other functions for a complete WMN-OAM set.

Understanding the difference between wired OAM and WMN-OAM is the unique challenge in a WMN OAM study. We continue to investigate the different characteristics and implement necessary tools to overcome these challenges. One example of these differences is co-existence of multiple networks in one location, while in case of wired networks, each network is isolated from others since they are separated. Multiple WMNs are exposed to each other due to sharing of an wireless medium, and therefore should develop simple solutions for any problems multiple co-existence.

6. Conclusions

In this paper, we introduced the concept of WMN-OAM to provide management functions in WMN, similar to OAM in wired networks with respect to different characteristics in WMN. We adopted a layered architecture for WMN-OAM and defined three domains; client domain, provider domain, and operator domain. We proposed a tree management model to handle WMN-OAM functions. In fault management, the provided functions are continuity check, loop back, and link trace. These functions detect, report, verify, and locate faults in the network.

The management approach provides an easy solution to handle mobility in WMNs, which is a problem that does not exist in wired network. It distinguishes between a client absence due to failure and due to movement with reasonable time bound. The model is general and applicable to any kind of WMN; furthermore, it is expected to provide scalability and cost low overhead.

We discussed performance management issues, to show the importance of monitoring and how we can utilize monitoring information. We proposed a performance management system to show how performance monitoring can be used to enhance performance. However, a further study should be done to implement a full performance management model and security management model.

References

[1] IEEE Std 802.1ag. http://ieeexplore.ieee.org/xpls/abs_all.jsp?tp=&isnumber=4431835&arnumber=4431836&punumber=4431834

[2] ITU-T Rec. Y.1731 "OAM functions and mechanisms for Ethernet based Networks", 2006.

[3] M. Kserawi, S. Jung, J. K. Rhee, "Wireless OAM for Securing Wireless Network Jamming Attacks", Proceeding of Triangle Symposium on Advanced ICT (TriSai), 2008, Daejeon, South Korea, pp. 253-255.

[4] S. L. Shrestha et. al. "An Open Wireless Mesh Testbed Architecture with Data Collection and Software Distribution Platform", Proceeding of 3rd international conference on Testbeds and Research Infrastructure for the Development of Networks and Communities (TridentCom), 2007, Orlando, United States, pp. 1-10.

[5] Firetide HotView Pro Mesh Management System, www.firetide.com

[6] BelAir BelView Network Management System, www.belairnetworks.com

[7] X. Cheng, P. Mohapatra, S. Lee, S. Banerjee "MARIA: Interference-Aware Admission Control and QoS Routing in Wireless Mesh Networks", Proceeding of International Conference on Communications (ICC) 2008, Beijing, China, pp. 2865-2870

[8] K. H. Kim and K. G.shin, "Accurate Measurement of Link Quality in Multi-hop Wireless Mesh Networks", Proceeding of 12th annual International Conference on Mobile Computing and Networking (MobiCOM), 2006, Los Angeles, United States, pp. 38-49.

[9] K. N. Ramachandran, E.M. Belding-Royer, K. C. Almeroth, "DAMON: A Distributed Architecture for Monitoring Multi-hop Mobile Networks", Proceeding of the 1st annual IEEE Communication Society conference on Sensor and Ad Hoc Communications and Networks (SECON), 2004, Santa Carla, United States, pp. 601-609.